



Insper

# **Ativos Digitais e Blockchain**

**Ricardo Rocha**  
**Raul Ikeda**

# Objetivo

- Discussão sobre cryptomoedas

# Relembrando

- Passada: Por dentro da tecnologia Blockchain
- Fundamentos de Macroeconomia
- Fundamentos de Finanças

# Bitcoin

- Cryptomoeda com a maior captação (\$180 bilhões<sup>1</sup>) e visibilidade
- Como já mencionado, criada em 2009 por S. Nakamoto
- Apresentou a tecnologia Blockchain
- Utilizada para transferência de valores eletronicamente e de forma descentralizada (sem um regulador governamental)
- Atualmente possui o tamanho de 264Gb (23/Fev/2020)

<sup>1</sup> fonte: <https://coinmarketcap.com/>

# Bitcoin – Histórico de Preços



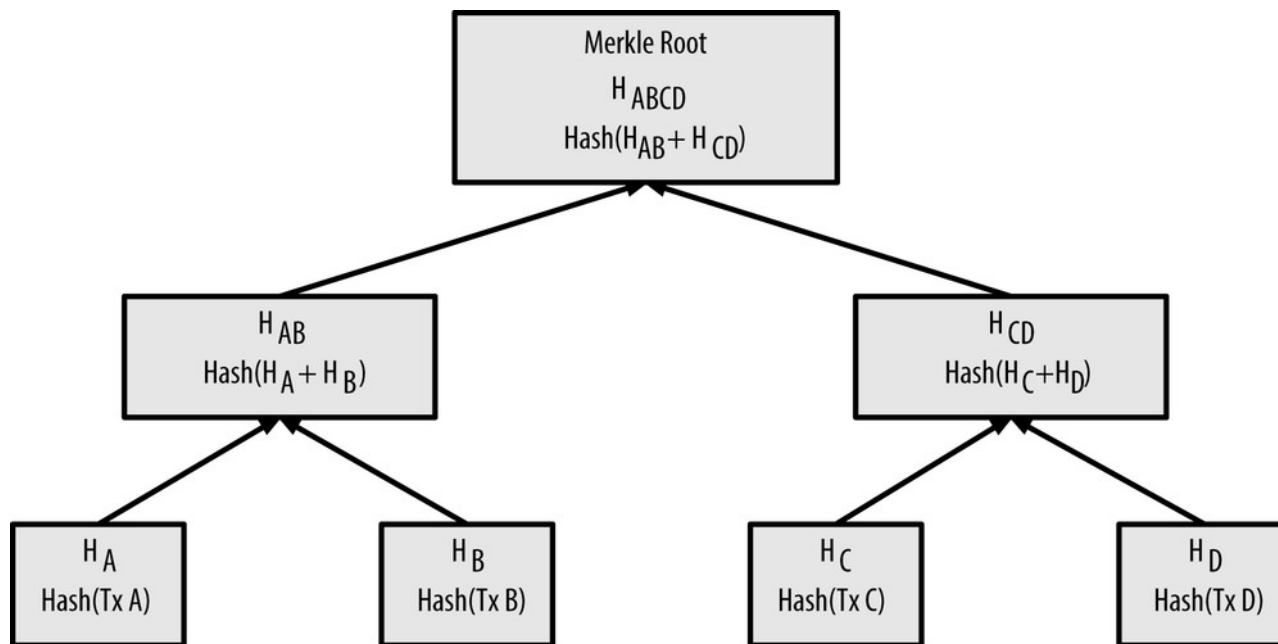
fonte: <https://www.blockchain.com/>

# Bitcoin – Tecnicamente...

- Usa SHA-256 como função de hash do bloco.
- Cada bloco possui uma variável target que indica a dificuldade de mineração.
  - Ao invés de atingir n zeros à esquerda do hash, basta que o hash seja menor que o valor target.
  - É recalibrada a cada duas semanas para que cada bloco seja minerado de 10 em 10 minutos em média.
  - Flutua de acordo com o esforço computacional de todos nós da rede.
- O hash é formado pela estrutura: hash do bloco anterior, target, nonce e hash da raiz da Merkle Tree das transações.
- Obs: existem dezenas de detalhes técnicos no bitcoin. Consultar o Antonopoulos para mais informações.

# Merkle Tree

- Árvore binária de hashes. Estrutura:



fonte: Antonopoulos, A. M., 2014

- Vantagens:
  - Fácil de verificar se a árvore está correta.
  - Fornece uma raiz com código único.
  - Não é preciso possuir todas as transações para validar uma transação.

# Transactions

- Funcionamento análogo ao discutido na aula anterior.
- Utiliza ECDSA para geração de chaves pública e privada.
- É possível fazer uma transação múltipla (1 para n)
- Cada transação gera um fee para o minerador do bloco.
- Muitas transações são rejeitadas.
- Para mais informações dos últimos blocos e transações:

<https://www.blockchain.com/explorer>



# Coinbase

- Inicialmente cada bloco remunerava o minerador em 100 bitcoins.
- A cada 210k blocos, a remuneração cai pela metade.
- Atualmente equivale à 12.5 bitcoins.
- Acredita-se que em 2020 sofrerá um novo corte.
- Estima-se que a partir de 2140, a remuneração será zerada e os mineradores ganharão apenas transactions fees.
- Haverá 21M de bitcoins no total.
- Acredita-se que parte dos bitcoins já estão perdidos e nunca mais serão movimentados.
- Pergunta: Existe anonimato no bitcoin?

# Wallets

- A base blockchain é apenas um livro-caixa.
- Todas as transações são listadas porém não estão consolidadas.
- Qualquer um que tenha uma cópia das transações consegue validar e consolidar o saldo de um endereço.
- O termo wallet é designado para representar uma carteira que contém as chaves privadas de um determinado endereço. Não contém moedas realmente.
- Pode ser implementada em hardware ou software.
- Existem empresas que administram carteiras.
- Você pode comprar e vender bitcoins diretamente na rede ou nas corretoras.

# Corretoras

- Uma corretora permite transacionar moedas entre carteiras
- Funciona analogamente à uma bolsa de ações, mas de cryptomoedas
- Fornece preço de compra e venda (com spread, claro)
- NÃO necessariamente está transacionando na rede global (?!?)
- Caso Mt. Gox: <https://coinsutra.com/biggest-bitcoin-hacks/>
- Caso recente:  
<https://gizmodo.com/crypto-exchange-says-it-cant-repay-190-million-to-clie-1832309454>

# Tipo de Nós



## Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.



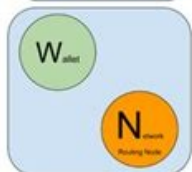
## Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.



## Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.



## Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.



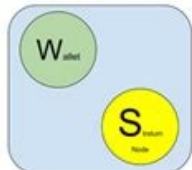
## Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.



## Mining Nodes

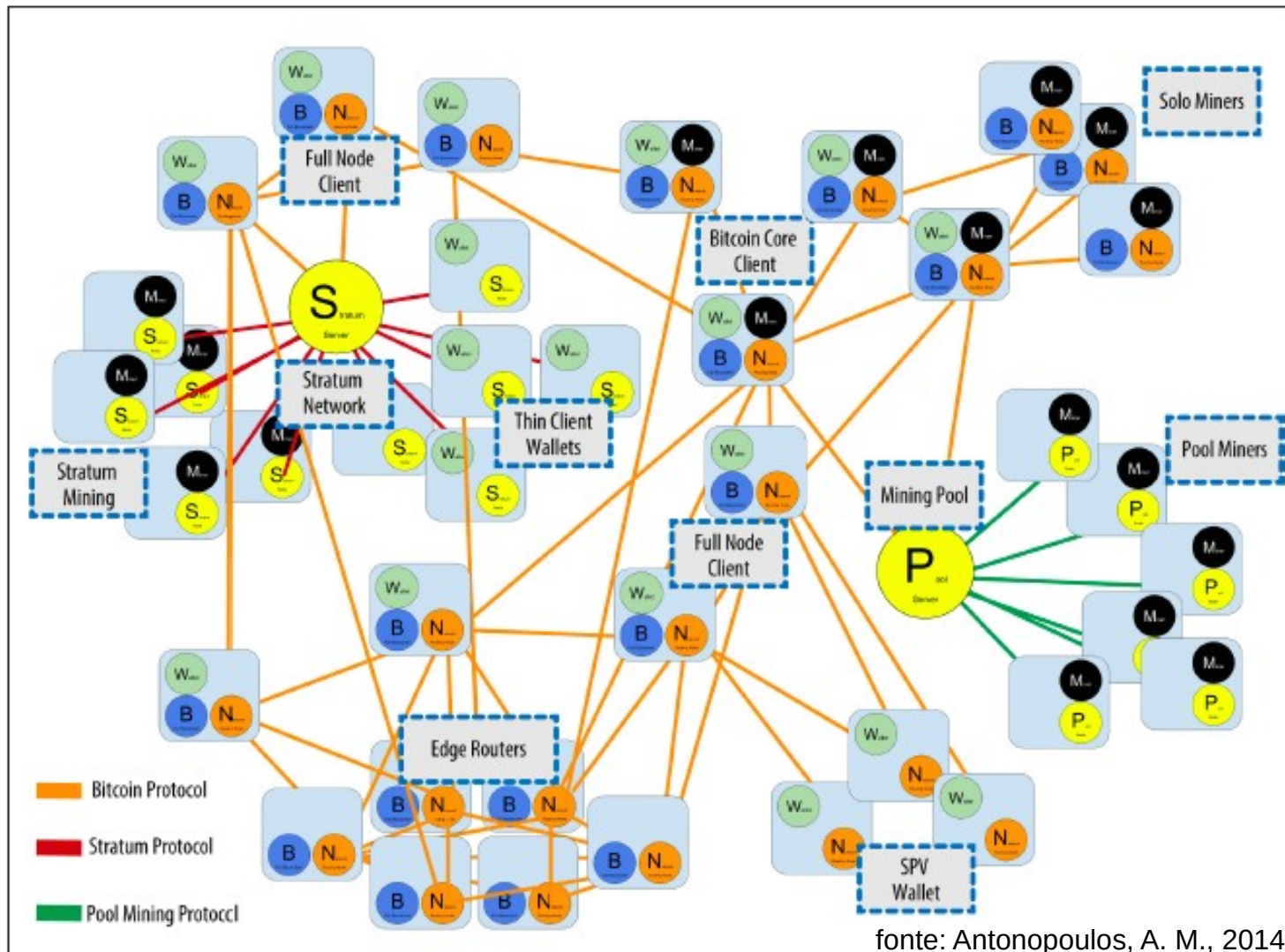
Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.



## Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.

# Exemplo de Rede



fonte: Antonopoulos, A. M., 2014

# BTC, XBT, BCH, BCG ou BSV?

- BTC é o código usual para bitcoin core, mas de acordo com a ISO 4217, o prefixo BT é reservado ao Butão. O correto seria usar o prefixo X de commodities. É a rede com maior captação.
- BSV (Satoshi Vision) mantém-se fiel à ideia original do paper.
- BCH e BCG são hardforks do BTC que alteram detalhes técnicos (por exemplo tamanho máximo do bloco ou algoritmo PoW), que redefinem os incentivos da rede.
- Na prática não há empecilhos para a realização de um hardfork, mas qual o impacto financeiro?
- Existem hardforks também em outras cryptomoedas.

Mais detalhes: <http://www.bitcoin-en.com/bitcoin-hard-forks-history.html>

# Implementação

- Bitcoin core: <https://github.com/bitcoin/bitcoin>
- Curiosidade: Bitcoin é considerado não Turing Completo. Mais detalhes no próximo slide.

# Bitcoin vs Ethereum

- Como visto bitcoin foi concebido para ser um livro caixa descentralizado.
- Imagine agora que ao invés de contas, você possua registradores. E que na verdade as transações são instruções para alterar esses registradores.
- Imagine ainda que seja possível programar esses registradores, configurando assim uma enorme máquina de estados.
- Esses programas são chamados de smart contracts e a rede que rege a execução desses programas é chamada Ethereum



# Ethereum - <https://www.ethereum.org/>

- Criado em 2014 por Vitalik Buterin (24 anos).
  - Um novo bloco a cada 15 segundos.
  - 3 ethers (moeda) por bloco minerado.
  - Quantidade ilimitada de ethers, porém com limite anual.
  - Usa uma EVM (Ethereum virtual machine).
  - Cada smart contract paga-se um fee para executar e/ou armazenar dados.
  - ASIC & FPGA safe – desenhado para rodar em computadores reais, com muita memória.
  - Segunda maior captação (\$20 bilhões)
  - Usa uma EVM (Ethereum virtual machine).
  - Blockchain size: 124 Gb (default), 3Tb (archive)
- 
- Não foi desenhado para ser rápido ou barato e sim confiável.
  - Possui uma gama de aplicações mais amplas que o Bitcoin.
  - Turing Completo

# Ether – Histórico de Preços



fonte: <https://www.blockchain.com/>

# Smart Contracts

- Bitcoin suporta apenas o registro de transações de moedas (livro caixa).
- Ethereum, por outro lado, permite a execução de programas com variáveis, loops, funções e eventos.
- É considerado um super computador descentralizado que armazena e modifica os estados de cada programa a medida em que as funções são chamadas.
- Esses programas são chamados de Smart Contracts.
- As aplicações formadas por smart contracts são chamadas de dApps (decentralized Applications)
- No Ethereum é necessário utilizar uma moeda chamada GAS para executar diversos comandos. GAS pode ser comprado com Ethers.

# PoW ou PoS

- Na aula passada foi apresentado o conceito de Proof-of-Work: o primeiro que descobrir o nonce do bloco, apresenta aos demais que validam o resultado.
- Proof-of-Stake apresenta uma ideia diferente: candidatos a mineradores realizam depósitos e o próximo minerador é sorteado proporcionalmente ao valor depositado. Caso o minerador cometa uma fraude, a diferença é descontada do seu depósito.
- Isso reduz significativamente o custo de mineração, tanto em equipamento quanto em eletricidade.
- Reduz significativamente o risco de ataque 50% + 1, pois não há incentivos para criar mining pools.
- Porém pode ser um sistema injusto se poucos participantes realizarem um depósito muito superior aos demais.
- Ethereum pretende migrar de PoW para PoS devido a problemas de congestionamento na rede.

# ETH ou ETC

- Em 2016 um fundo chamado The DAO, Decentralized Autonomous Organization, uma espécie de Kickstarter para Dapps, sofreu um grande ataque perdendo \$150 milhões devido a vulnerabilidade dos seus smart contracts.
- Após uma grande discussão, optou-se por reverter os blocos até o momento do início do ataque.
- Alguns membros achavam que modificar a Blockchain tiraria a sua credibilidade.
- Houve então um hard fork e criou-se a rede ethereum classic, que manteve a Blockchain intocada.

# Implementação

Site: <http://ethereum.org/developers/>















- Smart Contracts:
  - Solidity
  - Bamboo
  - Vyper
  - Flint
- Frameworks:
  - Truffle
  - Waffle
  - Brownie
  - etc
- Network:
  - Ganache
  - Ethnode
  - Infura
  - etc.

# Bitcoin vs Ripple

- Desenhado para ser um meio de pagamento e transferências completamente auditável
- Centralizado
- Alternativa ao SWIFT
- Pertence à uma empresa privada
- Não existe mineração, os blocos já foram minerados
- Transactions fees são jogados fora.
- 5 segundos de confirmação
  
- Dúvida: pode ser considerada uma cryptomoeda?

Etc...

## Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾							
Exchanges ▾ Watchlist							
USD ▾ Next 100 → View All							
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (
1	 Bitcoin	\$180.376.565.355	\$9.892,80	\$40.148.347.147	18.233.112 BTC	2,58%	
2	 Ethereum	\$29.869.266.962	\$271,98	\$19.325.896.477	109.820.124 ETH	3,72%	
3	 XRP	\$12.340.840.019	\$0,282080	\$2.328.324.057	43.749.413.421 XRP *	2,85%	
4	 Bitcoin Cash	\$7.262.304.655	\$396,97	\$3.989.008.357	18.294.338 BCH	5,58%	
5	 Bitcoin SV	\$5.331.195.827	\$291,45	\$2.190.800.308	18.291.690 BSV	3,29%	
6	 Litecoin	\$5.093.453.660	\$79,41	\$5.684.521.933	64.145.050 LTC	4,65%	
7	 Tether	\$4.654.379.338	\$1,00	\$46.879.094.491	4.642.367.414 USDT *	0,10%	

Mais detalhes: <https://coinmarketcap.com/>



# Reflexão

- Levando em consideração:
  - As particularidades apresentadas hoje e na aula passada
- Qual o futuro do bitcoin? E das cryptomoedas de modo geral?

# Próxima aula

- Separação da salas:
  - ADM/ECO: Python aplicado
  - ENG: Sistema Financeiro Nacional
- ADM/ECO: Instalar o Anaconda Python
  - <https://www.anaconda.com/distribution/>